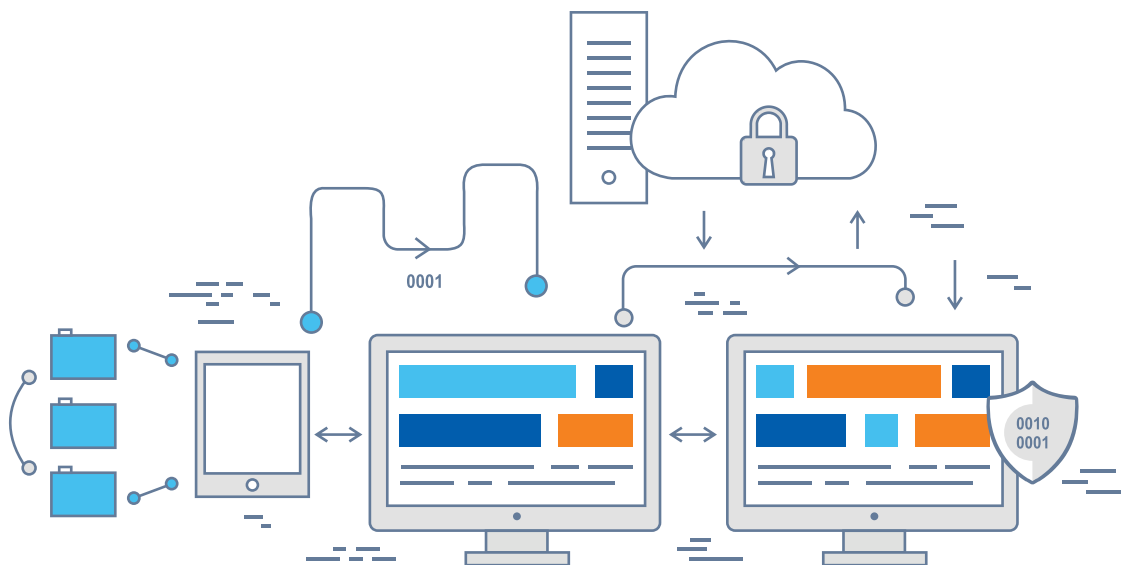




РОССИЙСКАЯ КОМПАНИЯ-РАЗРАБОТЧИК
КОМПЛЕКСНЫХ РЕШЕНИЙ ИТ-БЕЗОПАСНОСТИ «СМАРТ-СОФТ»

МЕТОДИЧЕСКОЕ ПОСОБИЕ

Информационная безопасность учащихся и соблюдение
законодательства РФ в учебном учреждении



2017 г.

СОДЕРЖАНИЕ

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАТИЗАЦИИ УЧЕБНЫХ УЧРЕЖДЕНИЙ.....	4
РАЗДЕЛ 1. ИНТЕРНЕТ В ЗАКОНЕ: ТРЕБОВАНИЯ, ОТВЕТСТВЕННОСТЬ, РЕШЕНИЯ.....	4
РАЗДЕЛ 2. ВСЕГДА В КУРСЕ: КАК ОБЕСПЕЧИТЬ ЭФФЕКТИВНЫЙ МОНИТОРИНГ СОЦИАЛЬНЫХ СЕТЕЙ.....	8
РАЗДЕЛ 3. СЕТЬ БЕЗ ПРОБЛЕМ: КАК ОРГАНИЗОВАТЬ ИНТЕРНЕТ- ДОСТУП В ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ. КОМПЛЕКСНОЕ РЕШЕНИЕ.....	11
РАЗДЕЛ 4. С ПОЛЬЗОЙ ДЛЯ ДЕЛА: КАКИЕ РЕСУРСЫ ПОМОГУТ В РАБОТЕ НАД ШКОЛЬНОЙ СЕТЬЮ.....	20
РАЗДЕЛ 5. ЕСТЬ ЛИ ЖИЗНЬ БЕЗ ИНТЕРНЕТА: О ПРОГРАММЕ «ТЕТРАДКА ДРУЖБЫ».....	22
РАЗДЕЛ 6. ВАЖНО ЗНАТЬ: ПРАВИЛА БЕЗОПАСНОСТИ ШКОЛЬНИКОВ В ИНТЕРНЕТЕ.....	25
О КОМПАНИИ.....	26
КОНТАКТЫ.....	27

Актуальные проблемы информатизации учебных учреждений

В Интернете сегодня множатся ресурсы, пропагандирующие суицид среди подростков. Роскомнадзор блокирует опасные сообщества. Но на месте одного закрытого открывается пять. Искоренить проблему пока не получается. Но есть возможность предупредить и избежать трагических последствий, если надлежащим образом контролировать присутствие подростков во Всемирной паутине, в том числе через школьную сеть.

Вместе с тем, есть проблемы, присущие информатизации российских образовательных учреждений вообще, которые существенно затрудняют выполнение этой задачи:

- не соблюдается законодательство, регулирующее доступ к Интернету и использование его несовершеннолетними;
- не ведется комплексный мониторинг пребывания детей в Интернете;
- отсутствует должная система защиты детей от информации, способной причинить вред их здоровью и развитию;
- нет централизованной системы аналитики для разработки мер профилактики суицида среди школьников.

Настоящее методическое пособие призвано помочь работникам сферы образования – чиновникам, директорам школ, учителям, а также родителям школьников понять, как избежать этих проблем и как сделать присутствие детей в Интернете безопасным.



1. ИНТЕРНЕТ В ЗАКОНЕ: ТРЕБОВАНИЯ, ОТВЕТСТВЕННОСТЬ, РЕШЕНИЯ

Правила и стандарты подключения российских образовательных учреждений к Интернету регламентируют следующие законы:

- ФЗ-436 «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- ФЗ-139 «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- ФЗ-149 «Об информации, информационных технологиях и о защите информации»;

- ФЗ-152 «О защите персональных данных»;
- ФЗ-188 «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»;
- Постановление от 31 июля 2014 г. № 758 об идентификации пользователей Wi-Fi.

Рассмотрим подробнее требования, предъявляемые законом, и решения, которые помогут администрации школы их соблюсти и тем самым избежать наказания.

ФЗ-139 и ФЗ-436 «О защите детей от информации, причиняющей вред их здоровью и развитию»

Требование. Российское законодательство обязывает администраторов точек публичного интернет-доступа использовать средства фильтрации, ограждающие детей от посещения ресурсов с опасным, экстремистским и порнографическим контентом.

Ответственность. При нарушении закона накладывается административный штраф: на граждан – от 2000 до 3000 рублей с конфискацией предмета административного правонарушения; на должностных лиц – от 5000 до 10 тыс. рублей; на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, – от 5000 до 10 тыс. рублей с конфискацией предмета административного правонарушения или административное приостановление деятельности на срок до 90 суток; на юридических лиц – от 20 тыс. до 50 тыс. рублей с конфискацией предмета административного правонарушения или административное приостановление деятельности на срок до 90 суток.

Решение. Блокировать ресурсы, не предназначенные для просмотра детьми. Это сайты, на которых пропагандируются наркотики, отрицаются семейные ценности, содержится нецензурная брань, информация порнографического характера, и другие ресурсы, указанные в законах, регламентирующих информационную безопасность детей.

ФЗ-152 «О защите персональных данных»

Требование. Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий.

Ответственность при нарушении норм, регулирующих обработку и защиту персональных данных работника: если у оператора будет выявлено 50 нару-

шений, каждое из них может быть квалифицировано отдельно, по каждому составлен протокол и за каждое наложен штраф от 25 тыс. до 50 тыс. рублей.

Решение. Использовать средства защиты – межсетевые экраны, сертифицированные ФСТЭК РФ по новым требованиям, вступившим в силу 1 декабря 2016 года.

В новых требованиях выделены следующие типы межсетевых экранов:

- межсетевой экран уровня сети (тип А) – применяется на физической границе (периметре) информационной системы или между физическими границами сегментов информационной системы;
- межсетевой экран уровня логических границ сети (тип Б) – применяется на логической границе (периметре) информационной системы или между логическими границами сегментов информационной системы;
- межсетевой экран уровня узла (тип В) – применяется на узле (хосте) информационной системы;
- межсетевой экран уровня веб-сервера (тип Г) – применяется на сервере, обслуживающем сайты, веб-службы и веб-приложения, или на физической границе сегмента таких серверов (сервера);
- межсетевой экран уровня промышленной сети (тип Д) – применяется в автоматизированной системе управления технологическими или производственными процессами.

Для дифференциации требований к функциям безопасности межсетевых экранов выделяется шесть классов защиты: от 6-го (низкий) до 1-го (высокий).

Межсетевые экраны, соответствующие 6-му классу защиты, применяются в государственных информационных системах 3-го и 4-го классов защищенности, в автоматизированных системах управления производственными и технологическими процессами 3-го класса защищенности, в информационных системах персональных данных при необходимости обеспечения 3-го и 4-го уровней защищенности персональных данных.

Межсетевые экраны, соответствующие 5-му классу защиты, применяются в государственных информационных системах 2-го класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 2-го класса защищенности, в информационных системах персональных данных при необходимости обеспечения 2-го уровня защищенности персональных данных.

Межсетевые экраны, соответствующие 4-му классу защиты, применяются в государственных информационных системах 1-го класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 1-го класса защищенности, в информационных системах персональных данных при необходимости обеспечения 1-го уровня защищенности персональных данных, в информационных системах общего пользования 2-го класса.

Межсетевые экраны, соответствующие 3, 2 и 1-му классам защиты, применяются в информационных системах, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну.

ФЗ-188 «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»

Требование. С 1 января 2016 года введен запрет на приобретение иностранного программного обеспечения для нужд государственных учреждений, за исключением тех случаев, если ПО соответствующего класса нет в едином реестре российских программ для ЭВМ и баз данных.

Ответственность. Отказ в праве проводить конкурс.

Решение. Работать с реестром отечественного ПО: <https://reestr.minsvyaz.ru/reestr>.

ФЗ-149 «Об информации, информационных технологиях и о защите информации»

Требование. Любая организация, предоставляющая доступ в Интернет, обязана блокировать ресурсы в соответствии с черным списком Роскомнадзора. У разных интернет-провайдеров обновление списков проходит не всегда своевременно, а ответственность ложится на компанию – организатора раздачи Интернета.

Ответственность. Нарушение требований настоящего закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность согласно законодательству Российской Федерации.

Решение. Использовать программное обеспечение для регулярной фильтрации по спискам Роскомнадзора. Как это сделать, вы можете узнать здесь: <http://www.smart-soft.ru/documents-useful-materials/roscomnadzor.pdf>.

Постановление от 31 июля 2014 г. № 758 об идентификации пользователей Wi-Fi и законопроект «О внесении изменений в Федеральный закон «О связи»

Требование. Предоставление доступа к сети Интернет в общественных местах осуществляется после идентификации оператором пользователей услуг связи и их оконечного оборудования. Идентификация может производиться по паспорту, учетной записи на сайте госуслуг или с помощью СМС-сообщения при авторизации.

Ответственность. Нарушение требований настоящего закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность согласно законодательству Российской Федерации.

Решение. Использовать программное обеспечение для идентификации пользователей по паспорту, учетной записи на сайте госуслуг или посредством авторизации с помощью СМС-сообщений.



Для проверки вашей школьной сети на соответствие требованиям закона, воспользуйтесь новым веб-сервисом

check.smart-soft.ru



2. ВСЕГДА В КУРСЕ: КАК ОБЕСПЕЧИТЬ ЭФФЕКТИВНЫЙ МОНИТОРИНГ ИНТЕРНЕТ-РЕСУРСОВ

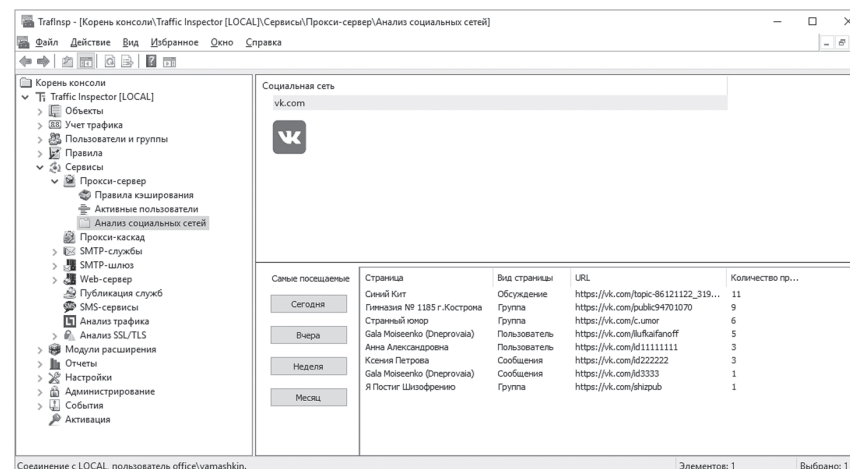
Для школьников доступ к Интернету со смартфонов давно стал каждодневной необходимостью. И если включенные в тарифный пакет мегабайты трафика стремительно улетучиваются, дети ищут возможность подключиться к открытой точке доступа Wi-Fi.

Подобные Wi-Fi-сети для публичного использования есть не только в метро и заведениях быстрого питания, но все чаще встречаются прямо в школах. И подростки не упускают случая воспользоваться ими: во-первых, бесплатно; во-вторых, быстро; в-третьих, нередко это единственный способ обновить страничку в социальной сети, отправить сообщение или просмотреть новости в любимом сообществе.

При этом администрация школы может получить доступ к статистике посещений и возможность анализировать весь спектр интернет-интересов

учеников. Обеспечить комплексный мониторинг пребывания детей в Интернете, в том числе осуществлять контроль за посещением ими ресурсов, пропагандирующих суицид, помогает сетевой экран, размещенный в пределах открытой сети.

В качестве примера рассмотрим возможности сетевого экрана Traffic Inspector. Функция мониторинга за социальными сетями в интерфейсе этого продукта представлена целым разделом.

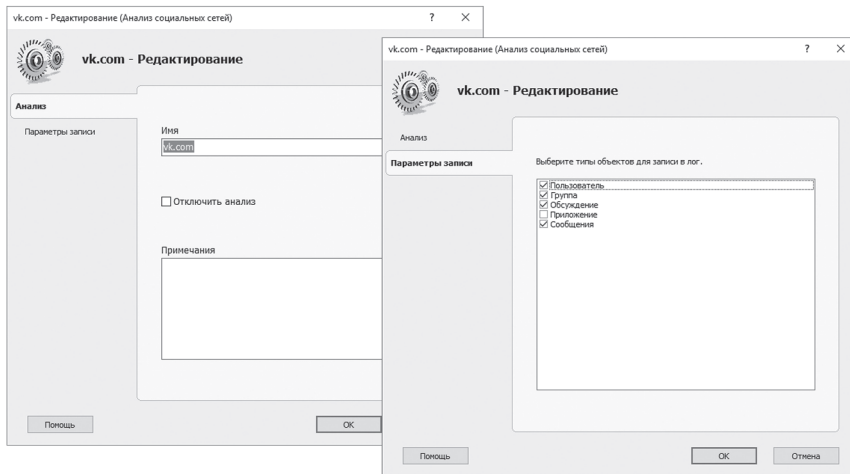


Консоль обеспечивает доступ к следующей информации:

- имена сообществ, групп и страниц – отчет по посещению учащими конкретными страницами социальной сети. Сетевой экран автоматически определяет типы страниц: группы, обсуждения, чаты или профили пользователей Сети;
- счетчик просмотров страницы – рейтинг часто посещаемых ресурсов;
- точный URL-адрес страниц – идентификация адресов сообществ и групп, доступ к постоянным ссылкам;
- точное время посещения – информация о том, когда посещались страницы;
- рейтинги за период – составление рейтингов самых посещаемых ресурсов за 24 часа, неделю, месяц.

На основе данных о количестве посещениях автоматически формируются рейтинги самых популярных сайтов. Сетевой администратор получает всю

необходимую информацию для дальнейшего анализа: тип страницы, имя сообщества или группы, URL-адрес.

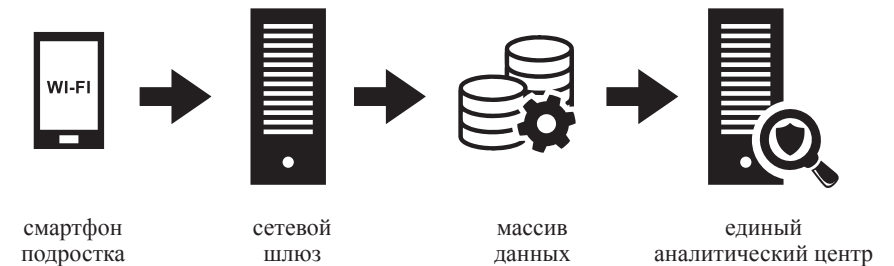


Перемещения по веб-страницам каждого подключенного к сети Wi-Fi школьника фиксируются в статистике сетевого экрана. Для систематизации полученной информации предусмотрены инструменты экспорта в виде наглядных таблиц.

Страница	Вид страницы	URL	Количество просмотров	
1	Психология	Обсуждение	https://vk.com/topic-8612136357	21
2	Синий Кит	Обсуждение	https://vk.com/topic-86121122_31938837	11
3	Киноманья	Группа	https://vk.com/public33692547899	10
4	Гимназия № 1185 г.Кострома	Группа	https://vk.com/public94701070	9
5	Дурь в голове	Обсуждение	https://vk.com/public36214588	9
6	Иван Эубов	Пользователь	https://vk.com/id98523641	7
7	Странный юмор	Группа	https://vk.com/fcurmor	6
8	Приколы да	Группа	https://vk.com/public2547896123	6
9	Приколист	Группа	https://vk.com/public36985236	6
10	Варья мозга	Обсуждение	https://vk.com/public21236925	6
11	Gala Moliseenko (Dneprovaia)	Пользователь	https://vk.com/luukalfanoff	5
12	В шоке	Группа	https://vk.com/public_2345698	5
13	Катя Смолина	Пользователь	https://vk.com/id36114425	5
14	Сергей Неклюдов	Пользователь	https://vk.com/id985223694212	4
15	Анна Александровна	Пользователь	https://vk.com/id11111111	3
16	Ксения Петрова	Сообщения	https://vk.com/id222222	3
17	Лучшие рецепты	Группа	https://vk.com/public369874256	3
18	Алена Иволгина (AIVA)	Сообщения	https://vk.com/id203638852	3
19	Ирина Люкшина	Сообщения	https://vk.com/id2036366258	2
20	Я постиг шизофрению	Группа	https://vk.com/shizpub	1

Пример сбора статистики в рамках одной из школ.

Сетевой экран позволяет понять, чем именно интересуются подростки, какие сообщества посещают чаще всего, с кем общаются, какие паблики открывают по несколько раз в день. Но самое главное, с помощью такого анализа можно обнаружить ресурсы, пропагандирующие суицид среди подростков.



Собранная статистика позволяет сформировать рейтинг опасных групп в социальных сетях, разработать их виртуальную карту и сделать борьбу с преступными сообществами по-настоящему эффективной. Информацию, полученную в результате мониторинга, можно использовать при разработке стратегии молодежной политики, направлений развития подростков с учетом их интересов.



3. СЕТЬ БЕЗ ПРОБЛЕМ: КАК ОРГАНИЗОВАТЬ ИНТЕРНЕТ-ДОСТУП В ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ. КОМПЛЕКСНОЕ РЕШЕНИЕ

Задачи по организации школьной сети в соответствии с законодательством РФ можно решить разными способами. Покупать отдельные программы, оборудование, тратить время на их интеграцию, настройку, поддержание работоспособности. Или приобрести комплексное решение Traffic Inspector School Edition, проверенное временем и клиентами, имеющее необходимые сертификаты, понятную документацию и обеспеченное технической поддержкой компании-разработчика.

TRAFFIC INSPECTOR

SCHOOL EDITION



Чтобы получить скидку при покупке Traffic Inspector School Edition, воспользуйтесь кодом купона



Инструкция для системного администратора по организации интернет-доступа в образовательном учреждении

С помощью этой инструкции вы сможете просто и быстро организовать безопасный Интернет в вашем учреждении.

Для организации интернет-доступа с нуля или модернизации IT-инфраструктуры школы в соответствии с действующим законодательством – ФЗ № 436 «О защите детей от информации, причиняющей вред их здоровью и развитию», №139 ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельными законодательными актами РФ по вопросу ограничения доступа к противоправной информации в сети Интернет необходимо выполнить все следующие пункты.

1. Подготовительные работы

На данном этапе необходимо произвести инвентаризацию имеющейся IT-инфраструктуры, разработать методологию систем маркировки, определить политику доступа к имеющимся службам и сервисам, учесть планируемые дополнительные сервисы.

По результатам инвентаризации появляется возможность судить о масштабе необходимой замены оборудования. При планировании закупок дополнительного оборудования рекомендуется придерживаться следующих советов:

а) со стороны структурированной кабельной системы: по возможности использовать управляемые свитчи с гигабитными портами и поддержкой технологии VLAN. Установить коммутационные шкафы на все точки расположения свитчей, в случае их отсутствия использовать патч-панели для коммутации, рассчитать количество LAN-розеток под каждого пользователя плюс на каждый кабинет иметь резервные розетки, промаркировать сетевые кабели;

б) со стороны серверной части: обязательно наличие хорошо вентилируемого безопасного помещения для организации в нем серверной. Минимальная серверная конфигурация должна включать в себя сервер шлюза, контроллер доменных служб и файловый сервер. Сервером шлюза может выступать решение DEPO Traffic Inspector, которое позволит организовать контроль доступа пользователей в сеть Интернет, а также соответствовать

требованиям производительности и безопасности. Контроллер доменных служб необходим для гибкого управления инфраструктурой, разграничения прав пользователей, а также для централизованного распространения требуемых политик безопасности. Файловый сервер рекомендуется для централизованного хранения пользовательских данных. Для доменных служб и файлового сервера рекомендуется использовать специализированные серверные решения или, в случаях ограниченного бюджета, обеспечить отказоустойчивость дисковой подсистемы RAID-массивом. Рекомендуется производить резервное копирование данных служб на отдельные NAS-серверы;

в) со стороны клиентов: убедиться, что установленные редакции поддерживают интеграцию в доменные службы Active Directory.

Соответственно, на данном этапе системный администратор должен определить текущие узкие места в IT-инфраструктуре школы, изучить текущие работающие сервисы локальной сети, разработать методологию для маркировки кабельных систем, для облегчения диагностики в случае возникновения проблем с СКС и согласовать бюджет согласно требованиям и возможностям руководства.

2. Проектирование политик IT-инфраструктуры, установка и настройка служб

Во время составления плана политик системному администратору необходимо разработать такую иерархическую систему, которая позволит охватить максимальное количество сходных пользователей минимальным набором правил. Данный подход позволит минимизировать количество дальнейших правок в уже рабочую инфраструктуру и обеспечить гибкость управления средой. Затем следует произвести установку или миграцию требуемых служб. Дополнительную информацию и пошаговые руководства по службам Microsoft можно найти по адресу <https://technet.microsoft.com/>. Также на данном этапе создаются необходимые учетные записи пользователей, групповые политики, иерархия файлового хранилища и его ACL-списков. Рассмотрим пример установки контроллера домена и создания ACL для общего ресурса.

1) Перед установкой роли контроллера домена необходимо настроить сетевой интерфейс целевого сервера, назначив ему статическую настройку IP и указать единственный адрес DNS-сервера как 127.0.0.1.

2) Устанавливаем роль «контроллер домена Active Directory».

3) После установки роли, если целевой сервер версии Windows 2008R2 – запускаем команду `dcpromo`, если 2012R2 – выбираем пункт «повысить до контроллера домена» в меню задач консоли управления сервером.

4) В открывшемся мастере указываем, что производим установку нового леса, – желаемое имя нового леса вида <любое имя>.local – режим функционирования домена и леса оставляем без изменений, на этапе мастера с указанием пароля для режима восстановления служб Active Directory вводим пароль, который будет использоваться для авторизации в режиме восстановления AD, на остальных шагах мастера значения по умолчанию оставляем без изменений. По завершении работы мастера потребуется перезагрузка.

5) На данном этапе переходим к созданию организационных подразделений, пользователей и групп. Для этого необходимо перейти в оснастку «Active Directory пользователи и компьютеры» либо же в окне «выполнить» написать: `dsa.msc`. Этап создания организационных подразделений и групп является довольно ситуационным и, как ранее было сказано, ответственным моментом, где необходимо заранее продумать иерархическую структуру, учитывающую логику IT-процессов школы. В дальнейшем для понимания базовых принципов мы рассмотрим упрощенный пример, когда мы создаем одно организационное подразделение для хранения одного пользователя и группы. В появившейся оснастке консоли создадим организационное подразделение (в иерархическом списке нажимаем ПКМ на корне текущего домена – «создать» – «подразделение» – в появившемся окне указываем имя подразделения (например, «персонал») и нажимаем кнопку «ок»). Выбираем в иерархическом списке наше созданное подразделение, нажимаем на нем ПКМ – «создать» – «пользователь» – в появившемся окне указываем данные пользователя, его имя входа – далее – указываем пароль пользователя, снимаем галку «требовать смену пароля при следующем входе в систему». По завершении работы мастера в нашем организационном подразделении будет находиться созданный пользователь. По аналогии создаем группу пользователей, где указываем ее имя, настройки группы в мастере оставляем без изменений. Добавим нашего пользователя в ново-созданную группу. Используем двойное нажатие левой кнопки мыши на целевой группе, в открывшемся окне выбираем вкладку «члены групп» – «добавить» – «дополнительно» – в графе имя указываем имя пользователя (или оставляем пустым) – кнопка «поиск» – двойной щелчок левой кнопкой мыши на целевом пользователе – «ок» – «ок». Таким образом, данная группа будет содержать целевого пользователя.

6) Теперь дадим этой группе ACL для доступа на расшаренную папку на файловом сервере.

Если файловый сервер еще не введен в домен, то вводим его через панель управления – «система» – в разделе «имя компьютера, домена ...» выбираем «изменить настройки» – в открывшемся окне кнопка «изменить» – переключить радиокнопку в положение домена и ввести имя домена нашей сети. Нажать в окнах «ок» и дождаться перезагрузки сервера. Теперь создаем на желаемом диске требуемую иерархию папок (в нашем случае

будет одна папка share на диске D) – нажимаем ПКМ на созданной папке – вкладка «доступ» – «общий доступ» – добавляем в список нашу целевую группу и указываем необходимые разрешения (например, чтение-запись) и нажимаем кнопку «поделиться». Теперь наша папка доступна по сети с заданными разрешениями.

3. Внедрение сетевого шлюза

Данная стадия включает в себя установку программно-аппаратного комплекса DEPO Traffic Inspector, импорт пользователей из базы Active Directory, создание групп, настройка правил сетевого экрана, правил ограничений для различных групп пользователей (например, учащихся и рабочего персонала). Для создания правил блокировки сайтов, указанных в государственном реестре для образовательных учреждений, необходима следующая последовательность действий.

1) В консоли администрирования, в иерархическом дереве Traffic Inspector, перейти в ветку «объекты» – «IP-сети» – «действия» – «добавить список». В открывшемся мастере на стадии автозагрузки ввести URL для загрузки http://list.smart-soft.ru/IP/zapretinfo_ip.txt и указать периодичность обновления с данного URL. Рекомендуемое значение – 1 раз в сутки в нерабочее время. Данный список будет включать IP-адреса запрещенных ресурсов;

2) В области «URL-списки» выбрать действие – «добавить список». Появится окно мастера, аналогичное предыдущему. На вкладке «автозагрузка» указать в поле «загружать с URL» адрес http://list.smart-soft.ru/URL/zapretinfo_url.txt. Данный список будет включать URL-адреса запрещенных ресурсов. Рекомендации по периодичности обновления – те же.

3) В разделе «правила» – «правила пользователей» иерархического списка консоли управления Traffic Inspector создать 2 запрещающих правила (в разделе мастера «тип правила» – «запрет»): одно с типом трафика «любой» и указанием в разделе «IP адрес» – «использовать список» – выбрать имя созданного списка в пункте «а») и второе – с типом трафика «трафик через прокси-сервер» с указанием в разделе «проверка URL» – «список» – выбрать имя созданного списка в пункте «б»). Далее необходимо сделать привязку данных правил к целевой группе учащихся, через меню настроек, пункт «правила группы до».

Детальный видеоурок по данному вопросу можно найти по адресу <http://www.smart-soft.ru/support/video/school>.

Для более гибкой фильтрации возможно использование модуля контентной фильтрации NetPolice, который предназначен для категоризации сайтов и

создания соответствующих правил для блокировки по критерию категории, настраиваемой в разделе создания правила «анализ контента» – пункт «проверка категории контента».

4. Настройка резервного копирования

Необходимо создать планы резервного копирования для каждого критического сервиса локальной сети либо же критически важных данных. Для доменных служб, в случае единственного контроллера домена, необходимо настроить полное резервное копирование и его периодичность (в зависимости от частоты правок базы Active Directory). Рекомендуется периодически проверять резервные копии на корректность.

5. Документация

Документация необходима для понимания IT-инфраструктуры школы. Поможет в быстрой адаптации новых сотрудников, ответственных за IT. В документацию рекомендуется внести схему текущей сети, используемое оборудование, описание схемы используемых политик, расписаний резервного копирования и другие данные, которые позволят за короткое время вникнуть в IT-инфраструктуру.



**Если у вас есть вопросы, обратитесь
в службу технической поддержки:**

 school@smart-soft.ru

 форум компании «Смарт-Софт»
forum.smart-soft.ru



Отзывы пользователей о работе с Traffic Inspector School Edition

“ Хотим отметить следующие достоинства работы данного проекта компании «Смарт-Софт»: бесперебойная работа локальной вычислительной сети в гимназии, блокировка нежелательных сайтов, безопасная работа в Сети всех учащихся и сотрудников, удобство пользования и настройки продуктов. Во время реализации безопасного доступа в Интернет учащихся гимназии № 8 команда специалистов проекта Traffic Inspector шла нам навстречу и тесно взаимодействовала с нашими сотрудниками. В гимназии были устранены все существовавшие проблемы с безопасной работой локальной вычислительной сети. Рекомендуем продукты компании «Смарт-Софт» к использованию в образовательных учреждениях и желаем новых успешных проектов»

С. В. Соколов,
директор МБОУ «Гимназия № 8»,
Московская область, г. Коломна.

“ Мы непрерывно используем решение Traffic Inspector в нашем образовательном учреждении на протяжении 7 лет. За это время значительно выросли требования к IT-инфраструктуре, ее защищенности и соответствию федеральному законодательству. Благодаря наличию интуитивно понятного интерфейса в сочетании с глубоко продуманной функциональностью продукта мы неоднократно рекомендовали к использованию данное ПО коллегам из нескольких образовательных учреждений»

В. А. Ковалева,
директор МБОУ «Талажская средняя образовательная школа»,
Архангельская область, п. Талаги.

“ Благодаря высокому уровню вашего профессионализма вместе нам удается выполнять очень важную миссию – обеспечивать успешное безопасное развитие и обучение подрастающего поколения!»

А. В. Добран,
директор МБОУ СОШ № 32,
Красноярский край, г. Норильск.

“ Уже 5 лет мы используем Traffic Inspector в своей школе и хотели бы отметить несомненные достоинства применения программы: экономия интернет-трафика, блокировка нежелательных сайтов и рекламы, простота и удобство пользования. Все это значительно улучшает образовательный процесс»

Ю. З. Яббаров,
директор КГАОУ «Школа космонавтики»,
Красноярский край, г. Железногорск.

“ Безопасность ребенка в школе – одна из наших первоочередных задач наравне с обучением и воспитанием будущего поколения. Пока ребенок находится в пределах образовательного учреждения, за его жизнь и здоровье, в том числе душевное, отвечает школа. Мы несем полную ответственность за учеников в любом пространстве, в том числе и информационном»

Спасибо за отличное решение: все настроено и полностью готово к работе. Продукт отлично справляется со всеми задачами, «незаметен» для нагрузки работы сети, функционален и надежен.

А. А. Аликов,
директор МБОУ «Гимназия № 2 Квантор»,
Московская область, г. Коломна.

“ Использование современных технологий в работе нашей школы привело к резкому расширению обращения к образовательным интернет-сервисам. В связи с постоянным подключением компьютеров к Сети, возникла необходимость высококачественной защиты от угроз и ограждения учащихся от нежелательного контента.

Traffic Inspector School Edition обеспечил нашему образовательному учреждению надежную сетевую защиту от вирусов, хакеров и спама. Решение максимально соответствует требованиям законодательства, фильтрует сайты с нежелательным контентом. Команда специалистов компании всегда готова оперативно ответить на все вопросы по работе с программой»

О. В. Кутовой,
директор МБОУ СОШ № 12,
Московская область, г. Коломна.



4. С ПОЛЬЗОЙ ДЛЯ ДЕЛА: КАКИЕ РЕСУРСЫ ПОМОГУТ В РАБОТЕ НАД ШКОЛЬНОЙ СЕТЬЮ

Сообщество взаимопомощи учителей

<http://pedsovet.su>

На портале можно найти нашу статью о том, как защитить школьную сеть от вредоносной информации без ущерба для учебного процесса:

<http://pedsovet.su/publ/44-1-0-5942>.

Горячая линия лиги безопасного Интернета

<http://hotline.friendlyrunet.ru/>

Горячая линия принимает сообщения о распространении в Сети интернет-материалов с порнографическим изображением несовершеннолетних. Обратиться сюда можно по телефону: +7 (499) 685-01-85, по электронной почте: info@FriendlyRunet.ru или через сайт.

Веб-сервис по проверке на соответствие законам

<http://check.smart-soft.ru/>

Чтобы избежать проверок правоохранительных органов, контролирующей организацию интернет-доступа в заведении, узнайте, нарушаете ли вы закон, прямо сейчас. Достаточно пройти по ссылке и через бесплатный веб-сервис попробовать открыть запрещенные ресурсы. Тем, кто предоставляет бесплатный доступ к Сети, – просто необходимо.

Противодействие пропаганде или вовлечению детей в группы для самоубийств

<https://www.oprf.ru/1449/2133/1474/2465/>

С помощью электронной формы обратной связи на сайте Общественной палаты РФ вы можете отправить ссылку на группу или аккаунт в «ВКонтакте», Facebook или Twitter, где идет вовлечение детей в группы, пропагандирующие

суицид. После экспертной оценки адрес ресурса будет передан в органы власти для блокирования, а содержащаяся в нем информация будет использована в разработке стратегии по пресечению противоправной деятельности.

Горячая линия РОЦИТ (региональная общественная организация «Центр интернет-технологий»)

<http://www.hotline.rocit.ru/>

На горячую линию можно сообщить о контенте, который, по вашему мнению, нарушает российское законодательство, а также о проблемах, связанных с предоставлением тех или иных услуг в Интернете (нелегальные/противоправные материалы, мошенничество, проблемы с интернет-сервисом – интернет-банкинг, интернет-магазин и пр.), низким качеством интернет-услуг.

Интернет-портфолио учителей

<http://www.bankportfolio.ru/>

Банк интернет-портфолио учителей. Международный проект.

Горячая линия Лаборатории Касперского

<https://newvirus.kaspersky.ru/>

Лаборатория Касперского традиционно занимается фактами распространения в Сети компьютерных вирусов. Обратиться в лабораторию за помощью вы можете как в электронном виде (по электронной почте: cert@kaspersky.com или через сайт), так и по бесплатному телефону: +7 (800) 700-88-11.

Федеральная служба по надзору в сфере защиты прав потребителей и благополучия человека

<http://rospotrebnadzor.ru/>

Как видно из названия, Роспотребнадзор выполняет функции по защите прав потребителей, а это значит, что обращаться сюда можно в случаях нарушения ваших прав со стороны российских интернет-магазинов. Прием обращений осуществляется в электронном виде.

5. ЕСТЬ ЛИ ЖИЗНЬ БЕЗ ИНТЕРНЕТА: О ПРОГРАММЕ «ТЕТРАДКА ДРУЖБЫ»



В 2016 году компания «Смарт-Софт» поддержала проект педагога Ольги Зубковой «Тетradка дружбы», считая его актуальным и важным. Уникальная технология, разработанная Ольгой Викторовной вместе со школьниками Пермского края, дает детям возможность активно общаться, проявлять свои творческие способности, заниматься социально-значимой деятельностью во внеурочное время и – что интересно – вне Интернета.

История создания. Авторы

Программа «Тетradка Дружбы» придумана в 2006 году. Автор – Ольга Викторовна Зубкова, педагог, международный эксперт по культурным программам Организации Объединенных Наций, автор более 100 педагогических разработок по вовлечению детей и молодежи в социально значимые формы деятельности, президент Национальной ассоциации «Тетradка Дружбы». Соавторами программы выступили школьники Пермского края, придумав компоненты технологии в формате «дети для детей». Поскольку в разработке программы участвовали дети, ее механизм прост и гениален в своей простоте. На сегодняшний день в программе участвуют более 1200 образовательных учреждений из 40 регионов России.

Актуальность программы

Еще совсем недавно родители могли с уверенностью доверить школе воспитание своих детей. До начала 1990-х школы России, гармонично сочетая обучение и воспитание, проводили системную работу по формированию разносторонне развитых и социально ответственных граждан страны. Однако после упразднения пионерии и комсомолии в качестве альтернатив-

ных полноценных государственных воспитательных программ, способных на долгий срок прижиться в школах, ничего предложено не было. В результате сформировалось целое поколение молодых людей, многие из которых замкнуты в своем внутреннем (зачастую виртуальном) мире, с низким уровнем общей культуры, с коммуникативными проблемами, с претензией на быстрые и нетрудоемкие результаты.

Пока взрослые думали, что сочинить взамен канувших в лету «идеологических» воспитательных программ, дети придумали способ объединения школьников независимо от возраста, успеваемости, социального статуса родителей, физических характеристик, возраста, географии проживания, национальности. Программа «Тетradка Дружбы» стала уникальной технологией для безграничного позитивного общения, детских социально-значимых инициатив и творчества в дополнение к учебному процессу.

Главный атрибут программы

Что может стать объединяющим атрибутом для взаимодействия всех детей в мире? То, что привычно, понятно и одинаково доступно всем детям. Таким атрибутом стала обычная школьная тетрадь. Простая ученическая тетрадка с логотипом и специальным дизайном, превратившись в «Тетradку Дружбы», сегодня выполняет функцию объединяющего атрибута для школьников образовательных учреждений из 40 регионов России, заменив собой пионерский галстук и комсомольский значок. Специальные тетради как обязательный элемент участия в детской долгосрочной программе выступают пропуском в мир разнообразных тематических мероприятий длиною в учебный год.

Роль «Тетradки Дружбы» в реализации программы

Все дети разные, поэтому подход к участникам программы индивидуальный, и тетрадки можно применить по-разному. Неуверенным в себе, закомплексованным, безынициативным ребятам предлагается рабочий вариант «Тетradки Дружбы» – просто для того, чтобы стать участником, членом большой команды детской социокультурной программы. Такие дети используют «Тетradки Дружбы» на уроках как обычные рабочие тетради (по русскому языку, математике, физике и пр.) Однако педагоги замечают, что именно в «Тетradках Дружбы» у ребят меняется почерк, у них появляется ответственность в выполнении домашнего задания, пропадает желание вырывать листы, неопытно вести записи, возникает заинтересованность в том, что будет дальше с этими тетрадками.

Ребята, которые хотят выразить свои таланты и способности, могут использовать «Тетradки Дружбы» в качестве творческих тетрадей. Участники программы могут поместить на страницах конкурсных тетрадей свои сти-

хи и рассказы, описать социальные проекты и культурные туристические маршруты по малой Родине, рассказать о традициях семейных чтений и пр. Часто к заполнению тематических тетрадей подключаются педагоги и родители. Таким образом, «Тетрадка Дружбы» становится универсальным средством самовыражения, коммуникации, творчества, диалога ровесников и людей разных поколений.

С целью реализации творческих инициатив участников программы, возможности общаться в живом режиме для детей, педагогов, родителей из разных городов и регионов России каждый месяц проходят разноформатные интерактивные мероприятия. Годовой цикл таких мероприятий позволяет поддерживать атмосферу постоянного живого творческого общения. Совместная деятельность детей, родителей и педагогов в процессе подготовки к мероприятиям создает условия для эффективного взаимодействия институтов семьи и школы при воплощении в жизнь социокультурных инициатив. Системная занятость участников программы в творческих, спортивных и других практиках решает проблемы профилактики негативных явлений, формирует в школах страны добровольческие отряды, службы примирения, патриотические клубы.

Знаковые события в истории развития программы

15 октября 2014 года в рамках форума ОНФ «Качественное образование во имя страны» президент России Владимир Путин отметил актуальность Всероссийской культурно-образовательной программы «Тетрадка Дружбы» и высказался в поддержку распространения «Тетрадок Дружбы» во всех школах России.

Программа получила широкое признание на международном уровне. «Тетрадка Дружбы» признана одной из лучших сетевых практик на конференциях в ООН «Добровольчество – технология социальных преобразований» (Женева, 2010–2015 гг.). Программа вошла в шестерку лучших социальных проектов на Международном форуме в поддержку Всемирного дня НКО (Хельсинки, 2014 г.). Генеральный секретарь ООН Пан Ги Мун лично познакомился с «Тетрадкой Дружбы» в рамках сессии ЭКОСОС Молодежного форума «Год возможностей для молодежи» (Нью-Йорк, 2015).

Перспективы

В январе 2017 года программа переросла в Национальную ассоциацию развития образования «Тетрадка Дружбы». Готовится к открытию сайт ассоциации. Пока с подробностями инновационной технологии можно познакомиться на сайте <http://www.тетрадкадружбы.рф>. Для всех, кто заинтересован в присоединении к новой организации, актуальная информация здесь: <http://тетрадка-дружбы.рф>.



6. ВАЖНО ЗНАТЬ: ПРАВИЛА БЕЗОПАСНОСТИ ШКОЛЬНИКОВ В ИНТЕРНЕТЕ

Памятка для подростков

- Нормы поведения и нравственные принципы одинаковы как в виртуальном, так и в реальном мире.
- Незаконное копирование продуктов труда других людей (музыки, игр, программ и т. д.) считается плагиатом (умышленное присвоение авторства чужого произведения).
- Не верьте всему, что вы видите или читаете в Интернете. При наличии сомнений в правдивости какой-то информации следует обратиться за советом к взрослым.
- Нельзя сообщать другим пользователям Интернета свою личную информацию (адрес, номер телефона, номер школы, любимые места для игр и т. д.).
- Если вы общаетесь в чатах, пользуетесь программами мгновенной передачи сообщений, играете в сетевые игры, занимаетесь в Интернете чем-то, что требует указания идентифицированного имени пользователя, тогда выберите это имя вместе со взрослыми, чтобы убедиться, что оно не содержит никакой личной информации.
- Интернет-друзья могут на самом деле быть не теми, за кого они себя выдают, поэтому вы не должны встречаться с ними лично.
- Нельзя открывать файлы, присланные от неизвестных вам людей. Эти файлы могут содержать вирусы или фото/видео с нежелательным содержанием.
- Научитесь доверять интуиции. Если что-нибудь в Интернете будет вызывать у вас психологический дискомфорт, поделитесь своими впечатлениями со взрослыми.



О КОМПАНИИ

Компания «Смарт-Софт» сегодня – это:

2 500 ПАРТНЕРОВ

Более 2 500 партнеров на российском и международном рынках

4 500 000 ЧЕЛОВЕК

4 500 000 человек работают в сетях, где установлены наши решения

14 ЛЕТ

14 лет на рынке информационной безопасности

3 АССОЦИАЦИИ

Экспертное членство в трех ассоциациях: АРПП «Отечественный софт», «Руссофт», Некоммерческое партнерство «Союз защитников информации»



КОНТАКТЫ

Звоните: +7 (495) 77-55-991

Пишите: school@smart-soft.ru

Заходите: www.smart-soft.ru

